São Paulo, 08 de maio de 2026.

PREGÃO ELETRÔNICO – PEE 202600024
OBJETO: "PRESTAÇÃO DE SERVIÇOS DE ENVIO, RECEPÇÃO E GESTÃO DE MENSAGENS NOS CANAIS SMS (SHORT MESSAGE SERVICE), RCS (RICH COMMUNICATION SERVICES) E WHATSAPP BUSINESS OFICIAL, PARA ATENDER ÀS DEMANDAS DAS ÁREAS DE NEGÓCIO DO SENAC, COM ABRANGÊNCIA NACIONAL"
ABERTURA: 13 DE MAIO DE 2026 – ÀS 10h00

CARTA ERRATA III

1. ALTERAÇÕES TERMO DE REFERÊNCIA

ONDE SE LÊ:

3.2 A Contratada deve possuir contratos diretos e homologados com as operadoras brasileiras autorizadas pela ANATEL para envio e recepção de SMS, garantindo rotas nacionais homologadas e proibindo rotas internacionais ou não autorizadas.

3.3 Para o canal RCS, a Contratada deve possuir contrato direto e homologação oficial junto à Google, incluindo os três níveis de RCS: basic, single e conversacional.

3.4 Para o canal WhatsApp, a Contratada deve ser BSP (Business Service Provider) homologado pela Meta (Facebook) para operação da API oficial, garantindo conformidade com as políticas vigentes da plataforma.

6.2 Em caso de rescisão motivada, o Senac poderá, além da multa prevista no item 17.1, aplicar à Contratada a suspensão do direito de licitar ou contratar pelo prazo não superior de 3 (três) anos.

LEIA-SE:

3.2. Para o canal SMS, a Contratada deverá garantir o tráfego por rotas nacionais homologadas, com vedação expressa ao uso de rotas internacionais/não autorizadas (rotas "cinzas"), assegurando rastreabilidade e entrega conforme requisitos do Termo de Referência.

3.2.1. Para atendimento ao item 3.2, a Contratada poderá:
a) possuir contratos diretos e homologados com operadoras autorizadas; ou
b) operar por meio de plataforma própria integrada a provedor de mensageria (broker/CPaaS), desde que a Contratada comprove documentalmente a regularidade

Gerência de Materiais e Serviços
Senac São Paulo

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
Tel.: 11 3236 2101
gms@sp.senac.br
www.sp.senac.br

dessa integração e a utilização de rotas homologadas, mantendo a responsabilidade integral pela prestação do serviço.

3.2.2. Em qualquer hipótese, permanece obrigatório o atendimento aos requisitos técnicos do canal SMS, incluindo integração, protocolos e relatórios previstos neste documento (ex.: SMPP/HTTP(S), DLR/relatórios e demais itens do 3.5).

3.2.3. As comprovações documentais relacionadas aos itens 3.2 e 3.2.1 serão exigidas para fins de homologação e início da execução do serviço, na forma definida pelo Senac.

3.3. Para o canal RCS, a Contratada deverá garantir operação com homologação oficial e suporte aos níveis RCS Basic e RCS Single, conforme requisitos deste Termo de Referência.

3.3.1. Para atendimento ao item 3.3, a Contratada poderá:
a) possuir contrato direto e homologação junto à Google; ou
b) operar por meio de plataforma própria integrada a broker/provedor homologado para RCS, desde que a Contratada comprove documentalmente a regularidade da integração e a homologação necessária para operação do canal (incluindo identificação do agente, quando aplicável), mantendo a responsabilidade integral pela prestação do serviço.

3.3.2. Para comprovação da condição de contrato direto junto à Google, ou da condição de broker/provedor homologado para RCS, a Contratada deverá apresentar evidência verificável por meio de captura/print do diretório público "Find a partner" do Google RCS for Business: https://rcsforbusiness.google/find-a-partner/

3.4. Para o canal WhatsApp Business Oficial, os serviços deverão ser prestados exclusivamente por meio da API oficial da Meta, em conformidade com as políticas e diretrizes vigentes, sendo vedadas soluções não oficiais (incluindo web scraping), números não oficiais ou gateways não homologados, conforme requisitos deste Termo de Referência.

3.4.1. Para atendimento ao item 3.4, a Contratada poderá:

a) ser BSP (Business Solution Provider) homologado pela Meta; ou
b) operar por meio de plataforma própria integrada a BSP homologado, desde que a Contratada comprove documentalmente a regularidade da integração e a oficialidade da operação do canal (incluindo evidência verificável quando aplicável).

3.4.2. Responsabilidade Em qualquer hipótese, a Contratada permanecerá integralmente responsável pela execução dos serviços, níveis de serviço (SLA), suporte, segurança da informação, rastreabilidade, conformidade com LGPD e demais obrigações contratuais.

3.4.3. Para comprovação da condição de BSP homologado ou de integração com BSP homologado, a Contratada deverá apresentar evidência verificável do status de parceiro (quando aplicável) e/ou declaração formal do BSP homologado que comprove a regularidade da operação e do vínculo/integração com a Contratada.

6.2 Em caso de rescisão motivada, o Senac poderá, além da multa prevista no item 17.1 do TGC, aplicar à Contratada a suspensão do direito de licitar ou contratar pelo prazo não superior de **3 (três) anos**.

2. INSERÇÃO DOS ITENS

3.10.12. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

3.10.12.1. Conformidade com a Lei Geral de Proteção de Dados.

3.10.12.2. Deverá adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito.

3.10.12.3. Os dados deverão ser protegidos por criptografia:
a) Em trânsito, utilizando protocolo TLS versão 1.2 ou superior;

Gerência de Materiais e Serviços
Senac São Paulo

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
Tel.: 11 3236 2101
gms@sp.senac.br
www.sp.senac.br

b) Em repouso, utilizando algoritmos reconhecidos de mercado (ex.: AES-256 ou superior).

3.10.12.4. Deverá garantir mecanismos de anonimização ou pseudonimização, sempre que aplicável.

3.10.12.5. Deverá manter política de segurança da informação, política de retenção e descarte de dados, previamente definida e alinhada com o SENAC.

3.10.13. CONTROLE DE ACESSO E AUTENTICAÇÃO

3.10.13.1. Implementar mecanismos robustos de autenticação, incluindo suporte a OAuth2, API Keys seguras e autenticação mútua (mTLS), HTTPS, conforme pontuado anteriormente.

3.10.13.2. O acesso aos sistemas deverá observar o princípio do menor privilégio e controle baseado em papéis (RBAC).

3.10.13.3. Credenciais e tokens de acesso deverão possuir prazo de expiração e política de rotação periódica.

3.10.13.4. Toda comunicação deverá utilizar exclusivamente HTTPS com TLS 1.2 ou superior, sendo proibidos protocolos inseguros ou obsoletos, garantindo também certificados válidos, configurações seguras de criptografia e proteção contra downgrade de protocolo.

3.10.13.5. Levando em consideração que os dados irão passar pelo ambiente da empresa, uma consideração é a possibilidade de usar uma VPN site to site. Esse tipo de conexão cria um túnel criptografado entre as redes das organizações, protegendo as informações contra interceptações, vazamentos e ataques cibernéticos. Além de assegurar a confidencialidade, a VPN também contribui para a integridade dos dados transmitidos e para a autenticação das partes envolvidas.

3.10.14. AUDITORIA, LOGS E RASTREABILIDADE

3.10.14.1. Manter registros (logs) detalhados de todas as operações realizadas, incluindo:
a) Envio e recebimento de mensagens;
b) Tentativas de autenticação;
c) Falhas operacionais e erros de processamento.

3.10.14.2. Os logs deverão conter, no mínimo: timestamp, identificador de correlação (correlationId), status da operação e identificação do evento.

3.10.14.3. Os logs deverão ser protegidos contra alteração e exclusão não autorizada.

3.10.15. GESTÃO DE INCIDENTES DE SEGURANÇA

3.10.15.1. Deverá possuir processo formal de gestão de incidentes de segurança da informação bem como plano de resposta a incidentes.

3.10.15.2. Incidentes que possam impactar dados ou serviços do Senac deverão ser comunicados imediatamente após sua identificação.

3.10.15.3. Fornecer informações detalhadas sobre o incidente, incluindo causa raiz, impacto e medidas corretivas adotadas.

3.10.15.4. Cooperar integralmente com o SENAC na resposta a incidentes.

3.10.16. SEGURANÇA DA APLICAÇÃO E INFRAESTRUTURA

3.10.16.1. Deverá apresentar gestão de vulnerabilidades com análises de vulnerabilidade e realização de pentest, incluindo conformidade com o OWASP Top 10.

3.10.16.2. A infraestrutura deverá seguir padrões de hardening e atualização contínua.

3.10.17. SEGREGAÇÃO E ISOLAMENTO DE DADOS

3.10.17.1. Garantir isolamento lógico entre clientes (multi-tenant), prevenindo acesso indevido entre ambientes.

3.10.18. CONFORMIDADE E AUDITORIA

3.10.18.1. Fornecer dados para auditorias de segurança ou evidências de conformidade.

3.10.18.2. Deverá ser fornecido relatórios de segurança, certificações ou evidências que comprovem a adoção de boas práticas quando solicitado.

3.11 DEFINIÇÕES

3.11.1. Provedor de mensageria (broker/CPaaS): empresa/plataforma que provê infraestrutura e integração para envio/recepção de mensagens em canais como SMS/RCS/WhatsApp.

3.11.2. Plataforma própria: solução tecnológica operada pela Contratada (ambiente, APIs, relatórios e gestão), ainda que utilize integração com provedor/broker homologado para execução do tráfego.

3.11.3. Rotas "cinzas" (SMS): rotas internacionais/não autorizadas, proibidas no TR (3.5.10).

3.11.4. API oficial (Meta/WhatsApp): integração formal da WhatsApp Business Platform, vedadas alternativas não oficiais.

COMISSÃO PERMANENTE DE LICITAÇÃO

Gerência de Materiais e Serviços
Senac São Paulo

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
Tel.: 11 3236 2101
gms@sp.senac.br
www.sp.senac.br